5 questions pour mieux comprendre le malware The Mask

En début de semaine, l'éditeur d'antivirus Kaspersky a publié un rapport mettant au jour un **malware hispanophone sévissant depuis 2007**, The Mask ou Careto. Les labos de l'éditeur ont dénombré 380 organisations victimes de ce malware sophistiqué, dans 31 pays. Quel que soit le mode de comptage (par nom ou par IP), **le Maroc, l'Espagne et la France** figurent parmi les principales victimes de cette attaque persistante (APT, pour Advanced Persistent Threat) visant à dérober des données à des gouvernements, des ambassades, des compagnies du secteur de l'énergie, du pétrole ou du gaz, des institutions de recherche, des fonds d'investissement et des activistes. *Silicon.fr* tente de répondre aux principales questions que soulève cette nouvelle menace très sophistiquée.

1) Quelle est la nature de la menace ?

Clairement, on ne parle pas ici d'un virus classique, mais bien d'une menace sophistiquée combinant **campagnes d'e-mails ciblés** (phishing) pour s'introduire au sein des organisations ciblées, utilisation de **nombreux exploits** pour pénétrer des systèmes et évolution au fil du temps. Kaspersky explique que les premières infections remontent à 2007. *« Nous sommes face à un malware évolué de type Duqu ou Gauss. En réalité, il s'agit de plates-formes d'espionnage persistantes*, analyse **Gérôme Billois**, senior manager en gestion des risques et sécurité chez Solucom. *Dans son approche, The Mask présente assez peu de nouveautés. On assiste en fait à un certain emballement médiatique, par exemple concernant le ciblage des terminaux mobiles sous Android et iOS. Le rapport de Kaspersky parle d'une ligne dans un log donnant à penser qu'un iPad a été victime de The Mask. C'est très léger pour tirer des conclusions générales, même si créer un malware pour iOS n'a évidemment rien d'impossible. »*

De son côté, **Marc Cierpisz**, en charge de la gestion des risques et de la gestion d'identités au sein de Devoteam, souligne : *« Le niveau d'élaboration de ce malware est assez élevé. The Mask a été conçu à dessein, pour récupérer de l'information, et a évolué avec le temps. »*

2) Quelles les caractéristiques marquantes de The Mask ?

Si The Mask amène peu de réelles nouveautés aux yeux des observateurs du secteur, il présente tout de même un certain nombre de particularités qui montre le **degré de raffinement atteint par les concepteurs** de cet APT. *« D'abord The Mask cible particulièrement les données utilisées pour le chiffrement ou la signature, preuve que les concepteurs de malware s'adaptent au renforcement de la sécurité dans les organisations visées*, remarque Gérôme Billois. *Ensuite, les assaillants ont anticipé la réaction des laboratoires et sociétés spécialisés en sécurité. En 4 jours, l'infrastructure de contrôle et commande de The Mask a disparu. Et ses concepteurs avaient prévu, dans les fichiers de configuration de leurs serveurs, de bloquer les requêtes venant des adresses IP des grands laboratoires et centres spécialisés. Ce qui montre qu'ils*

*étaient préparés aux investigations que leurs agissements allaient déclencher et qu'**ils avaient prévu un 'kill switch' en cas de découverte**. C'est un fait nouveau : jusqu'à présent les serveurs de contrôle et de commande des principaux malwares étaient souvent peu sécurisés*. » Cette anticipation visant à contrer les analyses des labos ne surprend par contre pas le CERT Devoteam (Computer Emergency Response Team, centres d'alerte et de réaction aux attaques informatiques, au nombre d'une dizaine en France), dont le directeur, **Sylvain Beck,** explique qu'il s'agit là d'un comportement qui se répand. Son collègue Marc Cierpisz note qu'il est *« probable que les concepteurs de ce malware aient prévu de le mettre en sommeil en cas de détection, afin d'analyser les réponses qui seront apportées par les antivirus pour être, demain, encore plus efficace. Le fait que The Mask soit aujourd'hui détecté n'est **pas du tout une garantie de son éradication**. Il est presque évident que ses concepteurs l'ont replongé en sommeil pour le retravailler. »* Pas franchement rassurant.

3) Qui est l'auteur de The Mask ?

Sur la base du niveau de sophistication du malware, **Kaspersky pointe clairement en direction d'un Etat** ou d'une structure pilotée par un Etat. L'emploi de l'espagnol au sein de The Mask / Careto est une autre particularité soulignée par l'éditeur d'antivirus. *« Les secteurs visés – ambassades, administrations, industriels de l'énergie – sont effectivement des cibles classiques des services de renseignement. En tout cas, il ne s'agit pas là des cibles habituelles des cybercriminels, dont l'objectif consiste avant tout à récupérer des données personnelles et financières »*, abonde Gérôme Billois, qui observe aussi *« l'intérêt très net des assaillants pour tout ce qui touche au Maroc. »*

Sylvain Beck et Marc Cierpisz, de Devoteam, sont, eux, moins convaincus par les conclusions de Kaspersky, qui ne fournit aucun élément probant à l'appui se son hypothèse. Marc Cierpisz remarque : *« **Le focus sur le Maroc pourrait être un leurre**, servant à détourner l'attention de la ou des véritables cibles de The Mask. »* Et d'ajouter : *« Contrairement à ce qu'affirme Kaspersky, ce n'est pas obligatoirement l'oeuvre d'un Etat. Il existe un marché de la faille. On peut commander la réalisation et l'orchestration d'un malware. Aujourd'hui, une grande entreprise pourrait très bien financer ce type d'attaque ciblée. »*

4) Quel rôle a joué la société française Vupen ?

Le **rapport Kaspersky cite nommément la société Vupen**, basée à Montpellier et notamment spécialisée dans la vente d'exploit (exploitation de faille) à des services de renseignement (Lire notre article, Prism : le révélateur du lucratif et très discret business de la vente de failles). The Mask repose pour partie *« sur au moins un exploit qui, selon la presse, a été vendue à des gouvernements comme un zéro day (exploitation de vulnérabilités non corrigée, NDLR) par la société française Vupen »*, écrit l'éditeur d'antivirus. Une **affirmation démentie par un tweet de Chaouki Bekrar**, le Pdg de Vupen, qui explique que l'exploit utilisé n'est pas celui de sa société et qu'il a probablement été conçu en analysant le patch publié par Adobe – l'éditeur concerné par la faille – après révélation de l'existence de la faille par Vupen.

La rédaction de *Silicon.fr* a contacté par email Chaouki Bekrar pour lui poser deux questions concernant cette position officielle publiée sur Twitter. Les voici :
– Est-ce que cela signifie que l'exploit que vous avez dévoilé n'a jamais été vendu à aucun de vos

clients ?
– Est-ce que cela signifie que vous avez-vous-même, au sein de Vupen, analysé les mécanismes employés par The Mask ?
Chaouki Bekrar n'a pas répondu précisément à nos questions se contentant d'indiquer : *« Nous n'avons aucune relation avec The Mask, pas plus qu'avec Stuxnet, Duqu ou Flame. Il existe plusieurs équipes de recherche compétentes à travers le monde capables de réaliser ce type de cyber opérations sophistiquées sans nécessairement faire appel aux services de R&D de Vupen. »*

Si on est donc **obligé de croire le Pdg de la société montpelliéraine sur parole**, Gérôme Billois note que *« l'explication fournie par Vupen est plausible. Par analyse différentielle, on peut concevoir un exploit à partir d'un patch. Et ainsi profiter de la fenêtre de vulnérabilité entre la publication d'un correctif et son application effective. Les entreprises les plus avancées mettent environ 48 heures pour appliquer un patch d'éditeur. Mais, dans la plupart des cas, cette durée atteint plutôt un mois ».*

5) Comment les entreprises doivent-elles réagir ?

La menace identifiée, que faut-il faire ? D'abord évidemment **vérifier si on a été victime du malware**, particulièrement dans les secteurs cités par Kaspersky dans son rapport. *« Dans ce rapport, l'éditeur décrit les indicateurs de compromission attestant de la réalité d'une infection dans une organisation donnée : IP, noms de domaine, fichiers. Ce sont des éléments clefs permettant aux entreprises de vérifier à posteriori si elles ont été touchées ou pas,* précise Gérôme Billois. *Les entreprises les plus avancées en matière de cybersécurité, disposant d'un CERT interne tenant à jour des listes de IOC (Indicators of compromise, NDLR), le font systématiquement. La difficulté ? Quand on trouve ces indices, il est souvent très difficile de remonter aux informations dérobées faute d'un système de surveillance suffisamment précis. »*

Pour Sylvain Beck, du CERT Devoteam, d'autres leçons doivent être tirées de l'affaire. En particulier **le rôle joué une fois encore par le phishing**, technique consistant à infecter des ordinateurs cibles via des emails conçus afin de pousser les utilisateurs à télécharger la souche infectieuse. *« Les entreprises devraient commencer par faire appel à des spécialistes de la lutte contre le phishing. Une autre réponse possible à cette multiplication des attaques ciblées réside dans le formatage régulier des machines des dirigeants des entreprises. Même s'il s'agit là d'un travail fastidieux et long. »*

Marc Cierpisz insiste, lui, sur la difficulté à éradiquer totalement un malware, même une fois l'infection détectée et isolée. *« Vous pouvez penser l'avoir détruit alors qu'en réalité, vous l'avez simplement replongé en sommeil attendant que ses concepteurs le réactivent »*, note-t-il. Avant de souligner le travail de fond que devraient mener les organisations françaises en matière de protection de leurs données sensibles. *« Sur le marché français, la prise de conscience des enjeux autour de ces questions reste bien trop faible. Et les entreprises en payent aujourd'hui les conséquences. »*

En complément :

– Toute l'actualité de la sécurité IT sur Silicon.fr